A Physics/Engineering of Failure Based Analysis and Tool for Quantifying Residual Risks in Hardware

Steven L. Cornford • Jet Propulsion Laboratory, California Institute of Technology • Pasadena
Mark Gibbel • Jet Propulsion Laboratory, California Institute of Technology • Pasadena
Martin Feather • Jet Propulsion Laboratory, California Institute of Technology • Pasadena
David Oberhettinger • Jet Propulsion Laboratory, California Institute of Technology • Pasadena

Key Words: Product Assurance Program, Risk Management, Defect – Characterization & Control, Physics Of Failure, Failure Detection & Isolation, Mission Essential, Test Program Set, Test Requirements, Tailoring, Cost Effectiveness

SUMMARY & CONCLUSIONS

NASA Code Q is supporting efforts to improve the verification and validation and the risk management processes for spaceflight projects. A physics-of-failure based Defect Detection and Prevention (DDP) methodology previously developed has been integrated into a software tool and is currently being implemented on various NASA projects and as part of NASA's new model-based spacecraft development environment.

The DDP methodology begins with prioritizing the risks (or FMs) relevant to a mission which need to be addressed. These risks can be reduced through the implementation of a set of detection and prevention activities—referred to herein as "PACTs (see Definitions). Each of these PACTs has some effectiveness against one or more FMs but also has an associated resource cost. The FMs can be weighted according to their likelihood of occurrence and their mission impact should they occur. The net effectiveness of various combinations of PACTs can then be evaluated against these weighted FMs to obtain the residual risk for each of these FMs and the associated resource costs to achieve these risk levels. The process thus identifies the project-relevant "tall pole" FMs and design drivers and allows real time tailoring with the evolution of the design and technology content. The DDP methodology allows risk management in its truest sense: it identifies and assesses risk, provides options and tools for risk decision making and mitigation and allows for real-time tracking of current risk status.

1. INTRODUCTION

NASA continues to make progress in response to its mandate to fabricate and operate spacecraft "faster, better, and cheaper" (Ref. 1). The posture of risk avoidance has given way to active risk management. A key element of NASA's risk management approach is to consider "risk as a resource" (Ref. 2). Like schedule, mass and power, risk is a resource to be traded against other resources and optimized subject to constraints. This process has been facilitated by the NASA focus on developing better risk management tools and methods (Refs. 3, 4, and 5). The DDP methodology (Ref. 6) and tool provides a "top down" approach to capturing requirements, estimating current risks, and making tradeoffs.

1.1 *Definitions*

The following technical terms are defined as they are used in the context of this paper:

Escape: An escape is a FM which was not detected or prevented by the application of one, or more, PACTs.

Failure: An event or condition that prevents a product or one of its constituents from performing an intended function. This may range from reduced gain of 1dB to an explosion, and may involve hardware or software.

Failure Mode (FM): The characteristic manner in which a failure occurs, independent of the reason for failure; the condition or state which is the end result of a particular failure mechanism.

Mission/Project Requirements: A set of characteristics or distinguishing features that are needed to meet operational needs and comply with applicable policy and practices.

PACTs: An acronym for "**P**reventative measures, **A**nalyses, process **C**ontrols and **T**ests," PACTs represent the set of all possible prevention and detection activities. As a product element passes through a PACT (e.g. a test), anomalies (FMs) are avoided (prevented) or observed (detected) and presumably fixed.

2. METHODOLOGY

2.1 Overview

In the project development process, Figure 1 illustrates the relative effectiveness of various activities in "screening out" defects. Each box in the figure represents a collection of

0-7803-5848-1/00/$10.00 © 2000 IEEE

PACTs, and the dotted lines represent "escapes"-- FMs that were not detected or prevented by that activity. The optimal implementation program is one that identifies and retains the minimum set of measures necessary to expose a critical failure or prevent it from occurring in flight.

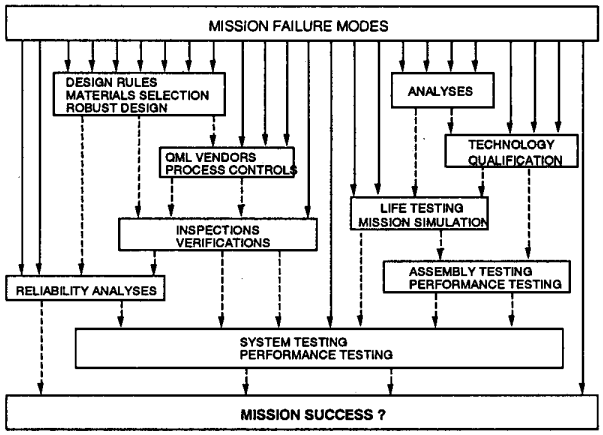

Figure 1. "Screening Out" the Defects (illustrative diagram—not to scale)

2.2 Four-Step Process

The DDP methodology consists of four steps. An ongoing example will be used to clarify the process. For simplicity this discussion will be constrained to two levels of hierarchy.

Step 1: Develop the Requirements Matrix. This step actually involves 3 sub-steps:

1. Identify the requirements (rows of the matrix),
2. Identify the FMs (columns of the matrix), and
3. Populate the matrix (the matrix elements).

This produces a prioritized set of FMs (risk elements) in which the "tallest pole" is (loosely) the FM which has the greatest impact on the most important requirements, and the "shortest pole" is the FM which has the least impact on the least important requirements. This prioritized set allows project personnel to focus their attention on a prioritized list of risk elements. Let us now examine in more detail how one achieves this critical result.

Step 1.1: Identify Requirements. This first step requires involvement from project personnel (the customers) and entails the identification, weighting and grouping of the requirements for the program or project under evaluation. This grouping may be by requirement type, or by the various instrument requirements, etc. The requirements are also weighted by the relative importance to the project. As an obvious example, the secondary mission requirements are weighted less than the primary mission requirements.

A simple example (Figure 2) illustrates a grouping into primary and secondary mission requirements. Under primary mission requirements, the weightings are all 10 except for the launch date, which is weighted as 8. Under secondary mission requirements, the weightings are 2 and 3, respectively.

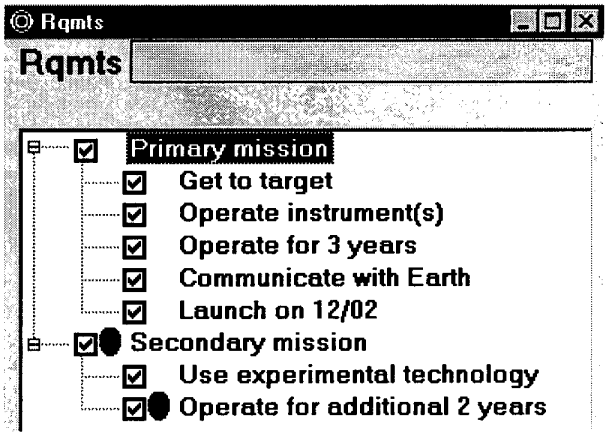

Figure 2. Sample DDP Output: Requirements Groupings

Step 1.2: Identify FMs. Next, the potentially relevant FMs (or risk elements) are identified and grouped (Figure 3). FMs may be identified by a variety of techniques including brainstorming, interviews with design engineers, or incorporating existing fault trees.

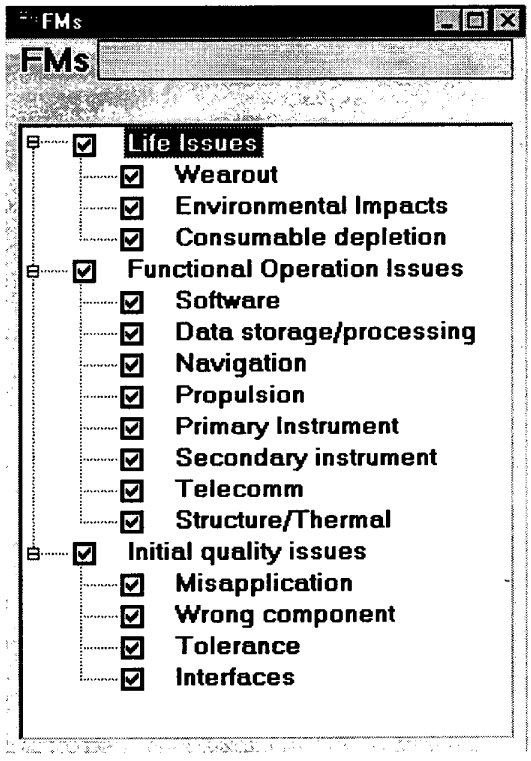

Figure 3. Sample DDP Output: Failure Modes

This identification and grouping is best done at a level consistent with the requirements. For example, the requirement "Operate for 3 Years" (Figure 2) leads one to worry about "Life Issues" (Figure 3). As the details of the design emerge, and the DDP process continues to stay synchronized with the project life cycle, the FMs start to become more specific and "Life Issues" is then broken into subordinate FMs (e.g. fatigue, expended consumables, environmental degradation) which will later be prioritized. This process is most easily and efficiently accomplished using a "critical mass" of experts since each discipline expert usually has a unique perspective, and experience indicates that many of the risk elements lie in the interfaces into which one person rarely has complete insight.

Step 1.3: Populate the Requirements Matrix. Now that the requirements and FMs have been identified, one can begin to evaluate the impact of each FM on each requirement. the percentage of each requirement lost should the FM occur is "scored" in the requirements matrix. At the higher levels of evaluation (such as those in this example), it is recommended to use a Taguchi-type non-linear scale. This is accomplished in Figure 4 by entering 0, 0.1, 0.3, 0.7 and 0.9 representing the fraction of the requirement impacted by the FM.

Figure 4 shows a portion of the (high level) requirements matrix generated using the previously identified FMs and requirements. The totals under the FMs represent the total impact and are used to perform the 'tall pole' assessment. The totals next to the requirements can be used to identify driving requirements, such as "Operate for 3 Years."

RxFM

RxFM 0 or empty = none lost 1 = 100% lost

		FMs				Functional Operation is		
		FMs	Wearout	Environm Impacts		Software	Data storage,	Ne
Rqmts	Rqmts	Totals	29.467	56.533		81.933	65.867	4
Primary mission	Get to target	116.33	0.1	0.7		1	0.3	
	Operate instrument(s)	121.67	0.1	0.7		1	1	
	Operate for 3 years	130	0.7	0.9		0.3	1	
	Communicate with Earth	115	0.1	0.3		1	0.3	
	Launch on 12/02	100				0.7	1	
	Use experimental technology	48.8	0.1	0.3		0.7	0.1	

Figure 4. Sample DDP Output: Requirements Matrix

Outputs of Step 1: One output of this step is a list of driving requirements (Figure 5). That is, the horizontal sum (for each requirement across all FMs) of matrix entries identifies the total extent to which a given requirement is "at risk" from the FMs. Since each requirement (and it's weight) ultimately drives the risk element priority, this output gives the project a chance to see which requirements were too aggressive or add no value. Note that generally any relaxation of requirements changes the FM impacts, which in turn reduces, or redistributes, the risk balance ("tall poles").

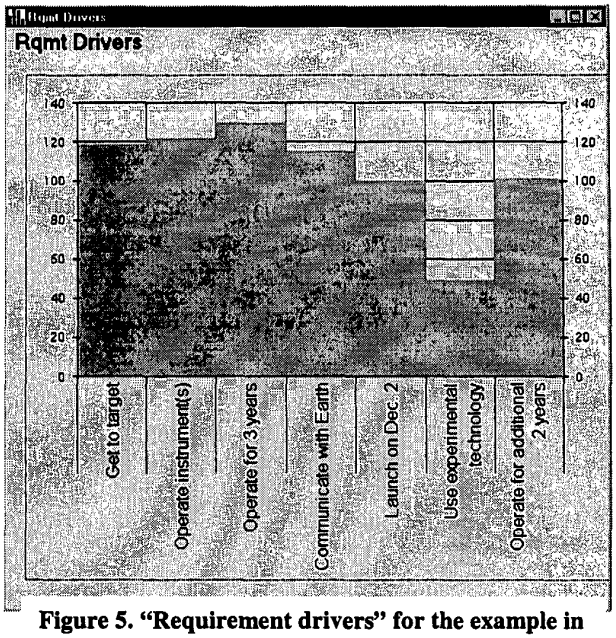

Figure 5. "Requirement drivers" for the example in the text. Note that the requirements most likely to be impacted by the risk elements can be easily identified.

As discussed above, Step 1 also results in a prioritized list (or Pareto diagram) of risk elements which can be used by various project personnel to focus their work. This collection of weighted risk elements (Figure 6) is also the key input to the next step. These represent the project risks and must be reduced to the desired levels.

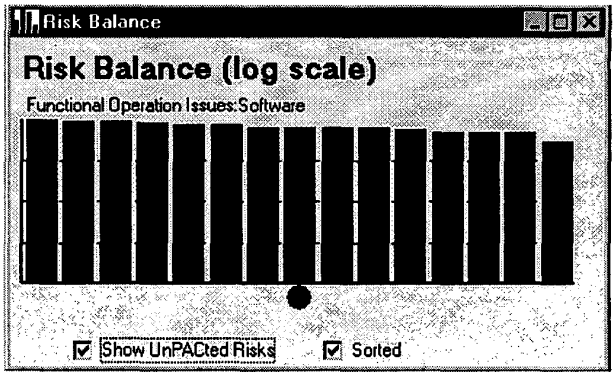

Figure 6 Initial risk balance for the example in the text. Note that no PACTs have been selected and the FMs are ordered according to total impact. The cursor (not visible) location is on the "tallest pole," which happens to be "Functional Operation Issues: Software" as the pop-up text indicates.

Step 2: Develop the Effectiveness Matrix. Now that we have identified and prioritized the relevant risk issues, we can begin

to explore possibilities for preventing or detecting them. This step really involves only two sub-steps since the FMs (columns) have already been identified in the previous step. These two sub-steps are (1) identifying detection and prevention options (PACTs) and (2) evaluating their effectiveness against the identified FMs. Obviously the more PACTs we do, the more we lower the risk, but each PACT has an associated resource cost (e.g., primarily mass for radiation shielding, but cost and schedule for radiation testing). There are thus optimal combinations of PACTs that fit the project resource constraints. Completion of the Effectiveness Matrix puts us in the position to tailor these activities.

Step 2.1: Identify the PACT Options. The list of PACT options is both long, and "pre-canned," in the DDP tool. Many of the usual PACTs at assembly level and above are very similar from project to project although they may be heavily tailored. The usual PACTs are already included in the tool (e.g., assembly-level thermal vacuum testing, system-level random vibration testing). Other PACTs are can be expressed generically, but can be made more project specific. For example, a project without optics would delete "Optical Testing" as a candidate PACT, while a project with optics would replace "Optical Testing" with something more specific such as "Optical Alignment Testing" and "Detector Calibration Testing."

The DDP tool is intended to assist the user in getting all of the PACT options "on the table" with names recognized by project personnel. In the early stages of the DDP process, it is better to have too many PACTs than too few, since the following steps will select or un-select the PACTs to see what subset produces the optimal solution.

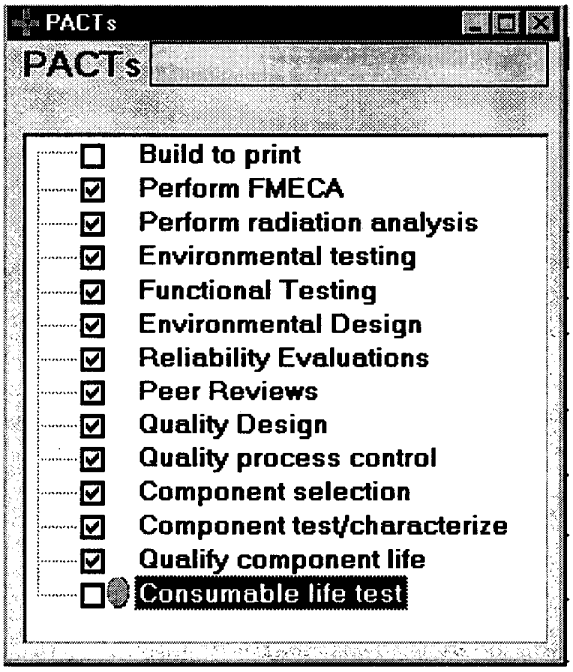

Figure 7. Sample DDP Output: PACTs

In Figure 7, The PACTs have been initially identified and a preliminary subset has been selected. Note that in this example, only "Build to Print" and "Consumable Life Test" have not been selected. As will be seen in the next graphic, this results in a low overall risk, but it is unbalanced and is inconsistent with the project resources.

Step 2.2: Populate the Effectiveness Matrix. Now that the PACT options are listed, the user evaluates (or reviews existing entries for) the effectiveness of each PACT on each FM (Figure 8). (Remember the FMs were entered when we completed the Requirements Matrix.) The default approach is to input the "effectiveness"; that is, the chance that the PACT will detect or prevent the FM from occurring. At the higher levels of evaluation (such as those in this example), it is recommended to use a "Taguchi-type" non-linear scale. This is accomplished by entering 0, 0.1, 0.3, 0.7, 0.9, and 1.0 representing the likelihood of the FM being caught the PACT. Thus, a 0.1 says that there is a 90 percent chance that the FM will not be caught. At lower levels of evaluation, more "digits of accuracy" may be appropriate, and there is a greater chance that such data will be available and applicable.

PACTxFM 0 = no escape, 1 or empty = 100% escape

	FMs				Functional Operation is			
	FMs		Environmenta impacts	Consumat depletion	Softw	Data store	Navic	Proj
PACTs	FoMRB		0.000010865	0.0098049	15485	4233	34071	1897
Perform FMECA	304.93		0.7	0.9	0.3	0.3	0.3	0.3
Perform radiation analysis	234.89		0.1			0.1	0.1	
Environmental testing	473.28		0.1		0.3	0.7	0.7	0.1
Functional Testing	544.45		0.9	0.1	0.01	0.01	0.1	0.7
Environmental Design	203.17		0.1			0.7	0.7	0.3
Reliability Evaluations	323.25		0.3	0.7	0.7	0.3	0.3	0.3
Peer Reviews	548.46		0.1	0.1	0.1	0.1	0.1	0.1
Quality Design	335.8			0.05	0.1	0.7	0.7	0.3
Quality process control	383.53			0.7	0.3	0.7	0.7	0.7
Component selection	448.76					0.1	0.1	0.3
Component test/characterize	157.32		0.1					
Qualify component life	108.73		0.1					

Figure 8. A sample output from the DDP tool which shows only a portion of the Effectiveness Matrix. Note that under the FMs is a # (expanded for the first two) which represents numerically the residual risk balance. Note that these first two FMs (among others) appear to be over-reduced (e.g. 0.000000035 is the probability of any of the various Wearout FMs escaping). But remember, this is the probability of all of the FMs that might have occurred not just those present after hardware delivery - the real goal is to get the lowest risk consistent with project resource constraints.

Outputs of Step 2: In addition to the residual risk balance after PACTs are applied (more about this in Step 3), Step 2 also provides a figure of merit for each PACT which represents the project relevant risk detected or presented by each PACT. This is the number to the right of the PACT name in the FMxPACT matrix (e.g. 548.5 for "Peer Reviews" versus 234.9 for "Perform Radiation Analyses").

Step 3: Tailor and Optimize the Risk Balance. Now we are in a position to access the heart of the DDP process: get the answer to the question "What to do on what?" Examination of the preliminary residual risk balance invariably reveals it to be very unbalanced. Some FMs have been disproportionately over-, or under-, addressed. Furthermore, the resource costs associated with the initial PACT selection are probably not consistent with project resource constraints. Thus, we begin selecting or un-selecting PACT boxes and examining the adequacy of the effect on the result. Selected PACTS affect the risk balance, unselected PACTS do not.

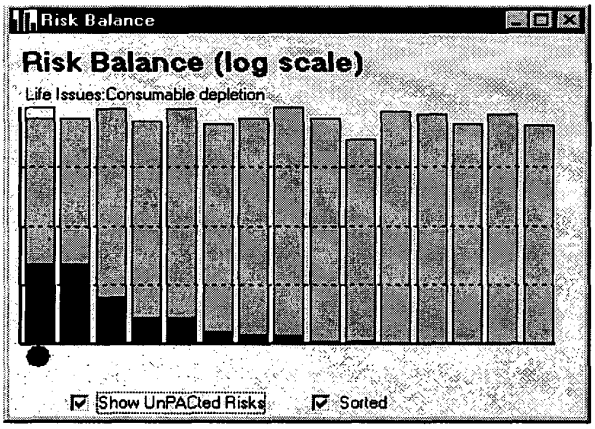

Figure 9. Illustration of the residual risk for the PACTs selected in Figure 7.

Note that some PACTs in Figure 9 have been solved into oblivion. The dark portion of the bar represents the portion of the risk NOT addressed, while others such as Consumable Depletion (column with the dot underneath) have been disproportionately under-addressed.

In Figure 10, an additional PACT (consumable life test) has also been selected. Consumable Depletion (the red dot) has been moved out of the top risk while others have moved up. The process continues until the project has the risk it desires within its resource constraints, or the project chooses a different implementation strategy. In the resolution of which PACTs to exercise one would go to lower-levels to tailor specific PACT applications to specific product elements.

been intentionally kept simple One could 'mix and match' PACTs on individual hardware elements with greater fidelity. However, this continuing example has so the user can understand the process and the role of the tool in this process.

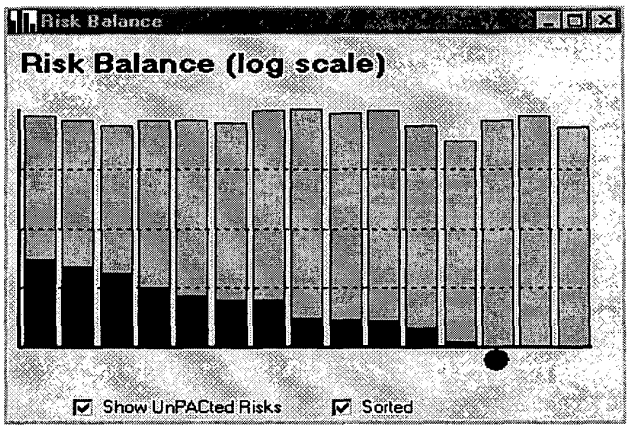

Figure 10. Illustration of the residual risk after a different combination of PACTs has been selected.

Step 4: Iterate with the Project Life Cycle. The FMs, requirements, and PACTs occur at various levels that range from mission level down to the device or semiconductor level. The DDP process is tailored to evolve with the project development cycle to allow risk elements to be identified as early as possible and remain consistent with the necessary initial allocation of resources and facility scheduling.

Thus, requirement trees begin with mission requirements but may branch down to box level performance requirements or lower. FMs may begin with "life issues" and branch down to "wearout" and then down to "insufficient lubricant". Similarly, PACTs may begin as an output of the NASA risk balancing profile (RBP) process (Ref. 5) and be implemented as specific tests or inspections on specific boxes. This process can go to lower levels, but this should mainly be used to resolve specific technical disagreements or make more complex/critical tradeoffs.

3. DDP IMPLEMENTATION

The generic DDP process steps have been described above. However, there are a number of subtle aspects to the DDP process which are discussed in the following paragraphs.

3.1 User Scenarios

Experience has shown that the initial population of the tool by a project is most effectively accomplished in real-time by a critical mass of experts. This first session is essentially a brainstorming session and is significantly enabled by electronic projection facilities (in which case the DDP tool is projected onto a screen for everyone to interact with). This process then includes a facilitator to keep the discussion moving and a clerk to capture the ideas generated.

Typically, the process starts with an introduction to the subsystem being evaluated. It then flows into identification of functions/requirements, followed by FM and PACT

identification and iterates to lower levels. The process terminates when the residual risk is acceptable.

3.2 *Iteration with the Project Life Cycle*

The DDP process also evolves to lower-levels of evaluation due to the project life cycle. As requirements are generated at lower levels, they are captured and the corresponding lower level risk elements (or FMs) are also listed. These usually result in lower level PACT selections (e.g. Testing versus Box A Functional Testing) as well.

3.3 *Creating Baselines*

The DDP tool allows the brainstorming to coalesce into a baseline, which can then be updated or modified in an individual or group setting. These modifications can then be merged and integrated into a new, better baseline.

3.4 *Integrating Existing Data*

Data from previous DDP evaluations can be "cut and pasted" into a new evaluation. Furthermore, since the underlying source of data for the DDP tool is contained in a relational database, data can be imported from Excel spreadsheets. Also, work has begun to attempt to import fault tree data directly from commercial software packages.

4. APPLICABILITY

Although the preceding example is a relatively high level "hardware" application, the DDP process has been applied successfully at varying levels of hardware integration (see Refs. 4 and 7). In fact, at lower levels of system integration, the requirements, FMs, and PACTs are often more clearly linked and more easily scored. Given the tool's tree structure, lower level assemblies can be rolled up to higher levels such that the tool can be used to span the entire manufacturing process cycle. Note also that the tool should be just as applicable for software as hardware.

5. ACKNOWLEDGEMENTS

The research described in this paper was carried out by the Jet Propulsion Laboratory, California Institute of Technology under a contract with the National Aeronautics and Space Administration through Code Q.

REFERENCES

1. *NASA Strategic Management Handbook*, National Aeronautics and Space Administration, Washington D.C., April 1996.
2. M. A. Greenfield and T. E. Gindorf, "Risk as a resource – A new paradigm", *Proc. ESREL 96 - PSAM III Conference*, Create, Greece, Vol. 3, pp. 1597, Springer-Verlag, Berlin, 1996 Jun 24 - 28.
3. L. Sarsfield, "The Cosmos on a Shoe String", MR-864-OSTP, RAND Critical Technologies InstituteWashington D.C., 1998.
4. S. Cornford, K.A. Hicks, "Evaluating the residual risks of infusing new technologies into NASA missions", *Proc. Ann. Reliability & Maintainability Symp., 2000 Jan.*
5. M. Greenfield, *Risk Balancing Profile Guide*, to be published in *the Proceedings of the 50th International Astronautical Conference*, 4-8 October 1999, Amsterdam, The Netherlands
6. T. E. Gindorf and S. L. Cornford, 'Defect Detection and Prevention (DDP): A Tool for Failure Mode Risk Management', to be published in *the Proceedings of the 50th International Astronautical Conference*, 4-8 October 1999, Amsterdam, The Netherlands
7. M. Gibbel and T. Larson, "Failure Engineering Study and accelerated stress test results for the Mars Global Surveyor sp[acecraft's power shut assemblies," Proc. InterPACK '99, Maui, 1999 Jun, p. 1389

BIOGRAPHIES

Steven L Cornford, *PhD*
Jet Propulsion Laboratory
M/S 303-217
4800 Oak Grove Drive
Pasadena, CA 91109-8099
E-mail: Steven.L.Cornford@jpl.nasa.gov

Dr. Steven Cornford graduated from UC Berkeley with undergraduate degrees in Mathematics and Physics and received his doctorate in Physics from Texas A&M University in 1992. He has served as a JPL Group Supervisor, Payload Reliability Assurance Program Element Manager, and as Principal Investigator for the development and implementation of the DDP software tool, including assisting JPL/NASA technologists in implementing a process for evaluation of early technology development efforts. He received the NASA Exceptional Service Medal in 1997 for his efforts to date. He is also the System Engineer for the New Millennium Program's Deep Space 3 interferometer.

Mark Gibbel
Gibbel Corp.
2550 Honolulu Avenue, Suite 201
Montrose, California 91020 USA
E-mail: gibbelcp@flash.net

Mark Gibbel graduated from California State Polytechnic University (Pomona) with a BS in Mechanical Engineering. He has been involved in design and test of advanced electronic packaging since 1977, when he developed the thermal models for Hewlett Packard's flip-chip technology. He has dedicated his professional career to developing and implementing failure physics-based test and verification methodology, with a particular interest in spaceflight electronics. Since 1985 he has been a member of the Reliability Technology Group within the Reliability Engineering Office of the Jet Propulsion Laboratory. He has managed numerous research projects within NASA's Test Effectiveness Program.

Martin S. Feather
Jet Propulsion Laboratory
M/S 125-233
4800 Oak Grove Drive
Pasadena, CA 91109-8099
E-mail: Martin.S.Feather@jpl.nasa.gov

Dr. Martin S. Feather obtained his BA and MA degrees in mathematics and computer science from Cambridge University, England, and his PhD degree in artificial intelligence from the University of Edinburgh, Scotland. For a number of years Dr. Feather worked on NSF and DARPA funded research while at the University of Southern California's Information Sciences Institute. He is currently a member of the Technical Staff at NASA's Jet Propulsion Laboratory. His research interests encompass the early phases of software development, especially requirements engineering and analysis/V&V.

David Oberhettinger
Logicon, Inc., a Northrop-Grumman company
2550 Honolulu Avenue, Suite 201
Montrose, California 91020 USA
E-mail: doberhettinger@logicon.com

David Oberhettinger manages the Spacecraft Engineering Technology Department (Logicon, Inc.) and is a member of the Reliability Technology Group at the Jet Propulsion Laboratory (JPL) in Pasadena, California. His present technical duties include participation as JPL representative to the NASA Reliability and Maintainability Steering Committee and as staff to the JPL Lessons Learned Committee, and assisting in microspacecraft reliability research. He also served as a vice chair on the RAMS2000 Management Committee.